Cassandra Crossing 627/ Dal pornocontrollo al tecnocontrollo

(627)—L'identificazione della maggiore età dei fruitori del porno è diventata legge senza che questo abbia creato reazioni significative…

Cassandra Crossing 627/ Dal pornocontrollo al tecnocontrollo



Figure 1:

(627)—L'identificazione della maggiore età dei fruitori del porno inizia a diventare legge senza che questo abbia creato reazioni significative. La SPID è stata dichiarata defunta dall'esecutivo, per essere sostituita dalla CIE. Sono fatti correlati tra loro? Certamente sono cattive notizie per i diritti civili digitali.

6 luglio 2025 —Chissà se altri, come Cassandra nel 2023 hanno aggrottato anche un solo sopracciglio alla notizia dell'approvazione del cosiddetto "decreto Caivano". Magari no, perché la notizia dell'obbligatoria verifica della maggiore età per i siti porno era dispersa in mezzo ad altre diverse e più ragionevoli questioni.

La realizzazione della verifica obbligatoria dell'età è andata avanti con tempi decisamente rapidi per gli standard italiani, probabilmente perché era in discussione anche in altri paesi europei.

In questa poco sana gara, la Francia ci ha battuto, attivandola per prima, salvo poi fermarsi, almeno temporaneamente, a seguito di una sentenza del tribunale amministrativo francese.

E' scesa infatti in campo una dot.com che non si era mai avvicinata molto ai riflettori, cioè Aylo, proprietaria dei principali (per non dire tutti) siti a luci rosse mondiali. Aylo sta trattando da pari a pari con gli stati nazionali e l'UE, come ci hanno abituato altre grandi e più note dot.com.

Aldilà dei dettagli, per quanto riguarda la libertà in Rete, impattata negativamente da qualsiasi nuovo obbligo digitale, la questione di Aylo è in realtà irrilevante.

Infatti nessuno degli attori coinvolti, nemmeno la stessa Aylo, mette in discussione la verifica obbligatoria dell'età, come fanno invece coloro che si occupano di diritti civili digitali. La questione su cui discutono è solo ***chi*** deve fare la verifica, se i siti, le piattaforme, od i produttori di device.

Per quanto riguarda il tecnocontrollo invece, basta dire che viene introdotta, ovviamente con la scusa di nobili fini, una nuova pastoia ed una limitazione dei diritti civili in Rete.

Una pastoia che, una volta resa obbligatoria, verrà senz'altro utilizzata per fini diversi e meno nobili.

Chi non condividesse questa facile profezia è invitato a ripassarsi la storia recente dell'introduzione della censura di internet in Italia, attuata tramite il ban di indirizzi IP e nomi di dominio. Anche questa era stata introdotta esclusivamente per nobili fini, ma si è poi estesa a questioni molto più mondane e terra terra di vari portatori di interessi, quali monopolisti della gestione di giochi di azzardo ed antispacciatori di pezzotti.

E certamente non è finita qui, perché, come recita un antico adagio, "*non bisogna preoccuparsi di quello che fa il governo di oggi, ma di quello che potrebbe fare il prossimo.*".

Ripetiamo, non si tratta di una buona notizia. Tutte le volte che viene istituita una limitazione generalizzata di una libertà digitale, tutte le volte che vengono istituiti nuovi obblighi che portano alle cessione di dati personali od a trattamenti di dati generalizzati all'intera popolazione, abbiamo tutti certamente perso una fetta di libertà in cambio di un dubbio vantaggio di sicurezza.

Da sempre infatti gli stati nazionali hanno la tentazione di controllare nella maniera più stretta possibile i propri cittadini. Negli stati "sani" questa "naturale" tendenza viene (più o meno) controbilanciata da altri organi dello Stato stesso, ma sopratutto dalle reazioni della società civile.

Sulla società civile, dopo l'avvento dei social, è il caso di stendere un velo pietoso. Concentriamoci invece su quello che è successo e sta succedendo in Italia in tema di digitalizzazione e tecnocontrollo.

Ma prima è necessario un veloce riassunto. Nella trentennale storia della digitalizzazione del nostro paese spiccano ben quattro storie di successo. Alcune addirittura di livello mondiale. Senza scherzi!

In ordine cronologico:

- [l'istituzione della firma digitale con valore legale parificato a quella autografa, primo paese al mondo;]
- [la creazione della Posta Elettronica Certificata, che permette di inviare messaggi con valore di raccomandata con ricevuta di ritorno, in maniera istantanea e sostanzialmente gratuita, invece che a botte di sette o più Euri;]
- [l'implementazione del Processo Civile Telematico, che solo chi frequenta da operatore i tribunali può apprezzare in tutto il suo valore;]
- [la realizzazione della SPID, un sistema di rilascio di credenziali con valore nazionale (no, non è un sistema di verifica dell'identità, checché se ne dica, e no, non ha nessuna vulnerabilità particolare).]

4 casi di successo della informatizzazione delle PP.AA. che decine di milioni di italiani ormai

utilizzano quotidianamente, a cui, solo per diffusione, se ne aggiunge un quinto, la CIE, Carta di Identità Elettronica.

C'è da dire che il "successo" della CIE è stato decretato ope legis come adempimento obbligatorio, supportato in maniera efficacissima dall'abolizione dell'alternativa cartacea, e solo dopo una trentennale ed iterativa gestazione sperimentale, che chi l'ha vissuta ancora ricorda nei propri incubi.

Senza altra volontà oltre quella di essere oggettivi, possiamo ricordare che Firma Digitale, CIE, CNS (Carta Nazionale dei Servizi), TSE (Tessera Sanitaria Elettronica) sono tutti tecnicamente in grado di fornire le funzionalità di identificazione, autenticazione e firma elettronica. La sola CIE possiede tuttavia lo status legale di documento di identità, che consente l'utilizzo come formale accertamento di identità.

Ora, potrebbe sembrare una cosa logica "accorpare" in un solo oggetto, la CIE, tutte le altre funzionalità, accentrando e "semplificando" una situazione che oggi, per quanto funzionante e largamente utilizzata, può apparire inutilmente complessa.

Sarebbe un errore; si tratta di una falsa semplificazione che, come tutte le soluzioni semplici di problemi complessi, è sbagliata. Cerchiamo di capire perché.

Chiunque abbia operato professionalmente nell'informatica sa perfettamente che la centralizzazione di qualsiasi cosa, se non fatta con estrema cura e professionalità e senza badare a spese, porta a vulnerabilità pericolose e potenziali, nuovi e gravi disservizi.

La storia, recente ed anche meno, dell'informatica nella pubblica amministrazione ci ha insegnato che il collasso di un intero sistema è cosa non potenziale ma reale, ed anche molto frequente.

Sistemi separati, quando cadono, tirano giù "solo" la loro funzionalità, senza compromettere tutti gli altri servizi. Se poi sono stati realizzati ridondati o federati, come la tanto vituperata ma ben progettata SPID, riescono a mantenere la propria funzionalità almeno in parte.

Cosa succederebbe invece se un ipotetico sistema "tuttologico", che fornisca firma, credenziali, autenticazione ed identità avesse un problema bloccante? E se, in questi tempi di guerra, questo problema bloccante fosse un atto criminale, oppure addirittura ostile?

Questo lungo antefatto ci è servito solo per arrivare finalmente alla cronaca di oggi.

Nel giro di pochi mesi, si è improvvisamente scoperto che la SPID è un sistema bacato e pericoloso, malgrado che 30 milioni di italiani la utilizzino quotidianamente al posto del più famoso e meno sicuro "1234", e che sia praticamente gratuita per le casse dello stato.

Si tratta anche qui di una notizia errata. Il rilascio di SPID multiple, quindi di credenziali multiple, non rappresenta di per sé un pericolo, anzi può essere utile per compartimentare le attività di una persona, separando ad esempio il privato ed il lavoro.

Il problema del rilascio di SPID ad impersonatori dipende invece dalle procedure di identificazione, che devono essere efficaci, che sono normate puntualmente e su cui lo Stato, per suo stesso regolamento, deve vigilare.

Contemporaneamente si è "scoperto" che la CIE può essere utilizzata, oltre che come documento di identità, anche come firma elettronica di tipo intermedio, e come credenziale di accesso.

Improvvisamente l'esecutivo, con un inusuale atto di decisionismo tecnologico, annunciato pubblicamente e ripetutamente, ha deciso di dismettere quello che è stato realizzato solo pochi anni fa e funziona, sostituendolo con qualcosa di ancora indefinito, di cui sappiamo solo che si

appoggerà alla CIE, tutto da realizzare e far adottare, ricominciando da capo un storia dolorosa, ma che era stata finalmente conclusa.

A Cassandra è venuta in mente la storiella dei frati che fecero pipì sulle mele piccole e brutte del loro albero, perché erano certi che ne sarebbero arrivate altre grandi e bellissime, e che quando queste non arrivarono dovettero mangiarsi quelle piccole e brutte.

Ecco, sembra proprio la storia della SPID, che una campagna di stampa poco informata, se non addirittura strumentale, ha definito "troppo complessa e poco sicura", raccontando che sarà presto sostituita dalla CIE inattaccabile e potente.

In tutto questo, cosa mai potrebbe andare storto?

Ci sono (purtroppo) altre chiavi di lettura che possono spiegare una vicenda apparentemente insensata sia tecnicamente che amministrativamente, riunirla all'improvvisa ed ineludibile necessità del *pornocontrollo* di stato, anzi a a livello europeo, e spiegare razionalmente tutto quanto.

Bastano due concetti chiave "*centralizzazione dei dati*" e "*tecnocontrollo dei cittadini*" per disegnare un panorama, anzi un vero progetto di controllo sociale, in cui la inspiegabile dimissione della SPID in favore della CIE diventa un elemento logico, razionale e necessario.

Infatti, se quello che si vuole ottenere è centralizzare il più possibile la gestione dei dati e degli accessi dei cittadini, con la conseguente possibilità di monitorare il loro operato, ed aprendo a teoriche ma terrificanti possibilità come quella di revocare completamente qualsiasi autorizzazione ad un individuo, allora sostituire un sistema federato e decentralizzato come la SPID con una gestione centralizzata, e dipendente da un documento emesso dallo Stato, è esattamente quello che serve.

E non è certo l'Unione Europea, con la sola eccezione del Parlamento Europeo, che potrà contrastare questo tipo di iniziativa, visto che la parte che conta davvero nel Trilogo, cioè la Commissione Europea ed il Consiglio di Europa, ormai da un decennio sta tentando di varare iniziative di tecnocontrollo a tutti i livelli, dal coordinamento degli organi investigativi nazionali fino al monitoraggio dei contenuti dei cellulari.

Se il nome Protect EU non vi è familiare, potete semplicemente considerare che la ben più famosa direttiva ChatControl ne rappresenta solo una piccola parte. ProtectEU è, per sua stessa definizione, una strategia quinquennale per rafforzare la sicurezza interna dell'Unione, anche attraverso nuove forme di controllo delle comunicazioni digitali.

Quindi anche attraverso il controllo delle comunicazioni dei cittadini europei, bypassando la "fastidiosa" crittografia dei device e la riservatezza delle comunicazioni.

Conviene quindi considerare gli scopi di ProtectEU, non solo in una meritoria ottica di contrasto alla criminalità, ma anche per il molto più importante effetto di compressione dei diritti civili presenti, e soprattutto futuri, dei cittadini dell'Unione.

In questa strategia di compressione delle libertà digitali, una parallela centralizzazione dei dati e delle autorizzazioni dei cittadini italiani appare perfettamente naturale ed integrata

Resta, a questo punto, da capire dove sia la convenienza per i cittadini europei nel permettere una operazione come questa, e se l'opposizione del Parlamento Europeo potrà tutelarli dagli effetti più deleteri di ProtectEU, come era riuscito a fare, anche se solo per un pelo, bloccando ripetutamente ChatControl.

Dato il panorama "digitale" di oggi, di cui fa parte sostanziale l'indifferenza del pubblico, non c'è davvero di che essere ottimisti.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra",
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

***Licenza d'utilizzo**: i contenuti di questo articolo, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link*.*

By Marco A. L. Calamari on July 14, 2025.

Canonical link

Exported from Medium on August 27, 2025.